

FILED

OCT 23 2019

JULIA C. DUDLEY, CLERK
BY: *A. Rust*
DEPUTY CLERK

UNITED STATES DISTRICT COURT

for the
Western District of Virginia

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

Hewlett-Packard Laptop (more fully described below)

Case No. 1:19mj145

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Black Hewlett-Packard (HP) Laptop with serial number 5CD3483WDF

located in the Western District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 18, USC, Section 401(3) and Title 18, USC 157	Contempt of Court and Bankruptcy Fraud.

The application is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[Signature]

Applicant's signature

SA David M. Britten

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/23/2019City and state: Abingdon, Virginia*[Signature]*

Judge's signature

Pamela Meade Sargent, U.S. Magistrate Judge

Printed name and title

5. This affidavit is made in support of an application for a warrant authorizing the search of stored electronic media and communications associated with the following laptop computer described as follows: Target Laptop 1 (TL1): a black Hewlett-Packard (HP) Laptop with serial number 5CD3483WDF. TL1 is a laptop computer owned by Patricia Geyer and used by Russell Louis Geyer. On 09/05/2019, Patricia Geyer voluntarily provided TL1, gave consent to search TL1, and signed a Consent to Search form.
6. Your Affiant respectfully submits that there is probable cause to believe that in the Western District of Virginia, Geyer, has violated Title 18, United States Code, Section 401(3) (Contempt of Court) and Title 18 Section 157 (Bankruptcy Fraud). Geyer knowingly disobeyed an order from the United States Bankruptcy Court to appear and testify at a hearing on September 5, 2019. Geyer communicated false and misleading information concerning his health status, location, and sale of collateral in the form of John Deere equipment, in order to mislead the court in the case of Russell Louis Geyer and Patricia Sue Geyer, Bankruptcy Case No. 18-71062; Deere & Company and John Deere Financial v. Geyer, Adversary Proceeding No. 18-07039. Your Affiant respectfully submits that there is probable cause to believe that Geyer may have used TL1 in furtherance of his bankruptcy fraud. Your Affiant respectfully submits that the search of stored electronic communications associated with TT1 will lead to the discovery of evidence of the above aforementioned offenses.

STATEMENT OF PROBABLE CAUSE

7. During a pre-trial conference on January 8, 2019, Attorney John Lamie provided to the court information given to him by his client, Russell Geyer. The information provided to the court stated that Geyer had gone to the Mayo Clinic in Florida for prostate surgery, complications developed, and cancer spread to his bones. Mr. Geyer intended to stop treatment and return home.
8. On May 16, 2019, information provided from Russell Geyer to Lamie caused Lamie to file a motion with the court to continue the trial set against Russell Geyer, where Deere & Company were requesting a judgement for the return of collateral from the Russell Geyer. In the motion Lamie asserted that Russell Geyer was in hospice care in Florida after the cancer treatment had failed. Patricia Geyer was also in Florida to be with her husband while under hospice care. Patricia Geyer suffered cardiac issues while there and recently underwent bypass surgery, and because of the bypass surgery, Patricia Geyer was not released to drive her vehicle back to Virginia.
9. On September 4, 2019, a subpoena was issued from the United States Bankruptcy Court in the Western District of Virginia, which commanded the appearance of Russell Geyer at a hearing on September 5, 2019. Attorney John Lamie instructed process server Kenneth Price to serve the subpoena on Russell Geyer.
10. During the afternoon of September 4, 2019, Price did serve Russell Geyer with the subpoena. After Price arrived at the residence located at 487 Still House Hollow Road, Saltville, Virginia, he observed a white truck, but no one was home. Just prior to leaving,

Price observed a small vehicle arrive. A male exited the vehicle and identified himself as Russell Geyer. Price served Russell Geyer with the subpoena.

11. On September 5, 2019, SA Childers was present in the United States Bankruptcy Courtroom, and observed that Russell Geyer had not appeared to testify as directed in the subpoena.
12. On September 5, 2019, Patricia Smith Geyer was interviewed, and stated that Russell Geyer was located at their personal residence, 487 Still House Hollow Road, Saltville, Virginia, prior to her leaving for the 10:30am court hearing. Russell Geyer said he would be leaving for court in a few minutes, and instructed Patricia Geyer to tell the truth if she was called to testify. Patricia Geyer stated that Russell Geyer did not have cancer, and that she had not travelled to Florida anytime in the last year.
13. On September 13, 2019, Patricia Smith Geyer was interviewed, and provided information that she was present on September 4, 2019 when Russell Geyer exited their vehicle and took possession of paperwork from an individual driving a black truck. Russell Geyer said the documents were related to their court hearing.
14. Patricia Geyer has never been admitted to a mental health institution, nor has she had bypass surgery on her heart.
15. A couple of days prior to the September 5, 2019 court hearing was the first time that Patricia Geyer had spoken to Attorney John Lamie. Lamie left a message for her at her place of work, and she returned his call. During their conversation, Lamie informed her that he had been told that Russell had died of cancer.
16. Since September 5, 2019, Patricia Geyer has received text messages from Russell Geyer stating that he was admitted to a hospital located in Charleston, West Virginia, after trying to commit suicide.
17. On 09/23/2019, pursuant to an arrest warrant issued in the Western District of Virginia, Special Agents of the Federal Bureau of Investigation and along with a Deputy United States Marshal, located and arrested Russell Louis Geyer date of birth (DOB) 08/16/1969, SSN 264-77-6259, at Abingdon, VA.
18. After his arrest on 09/23/2019, Geyer was advised of his Miranda Rights by SA Britten as read directly from a FD-395 Federal Bureau of Investigation Advice of Rights Form. Geyer said he understood his rights and said that he wanted to speak with SA Britten and SA Childers without a lawyer present. Geyer was provided with a FD-395 Federal Bureau of Investigation Advice of Rights Form and signed same. After being advised of his Miranda Rights and signing a waiver of those rights as documented on the FD-395 Federal Bureau of Investigation Advice of Rights Form; and after being advised of the identity of the interviewing Agents and the nature of the interview, Geyer provided the following information:

- a. Geyer said there was no one else involved; there was no other woman involved.
 - b. Geyer used an application called "incognito" to "spoof" his voice as that of a female and to change his telephone number when he contacted his attorney, in order to appear to be Patricia. Geyer said the "incognito" application would allow someone to change the appearance of their telephone number and the sound of their voice to that of a female or another voice in order to conceal the true number and sound of the caller.
 - c. Geyer said he sold the John Deere equipment to buyers in Kentucky and Tennessee.
 - d. Geyer admitted to fabricating an email from Attorney Jack Pankow in which he tried to implicate that Pankow sold the John Deere equipment and that he had instructed Geyer to kill himself.
19. In addition to the fabricated email referenced in paragraph 18.d. above, there are several communicated emails dated from November 2018 to August 2019 believed to be from Russell Geyer to Attorney John Lamie. From these emails, it is believed that Russell Geyer posed as himself, Patricia Geyer, and his brother in law, Robert Robbins. Through these series of emails, Russell Geyer communicated to Lamie that he was sick and hospitalized, that Patricia Geyer was sick and hospitalized, and that his brother in law, Robert Robbins, was attempting to obtain keys in order to return John Deere equipment. Based on my training and experience, it is believed that these aforementioned emails were an attempt by Russell Geyer to fraudulently delay and, or dismiss his bankruptcy hearing thereby committing bankruptcy fraud.
20. Investigation of allegations of Contempt of Court (Title 18, United States Code, Section 401(3)) and Bankruptcy Fraud (Title 18 Section 157) are matters within the jurisdiction of the executive branch of the Government of the United States.

LOCATION TO BE SEARCHED AND THINGS TO BE SEIZED

21. The information described in Attachment A will be subject to seizure by law enforcement.
22. Forensic Imaging

An important step that is ordinarily part of an expert's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. This could also require authorities to do on-site examination of the computer systems in order to document any volatile data. Examples of volatile data include, but are not limited to, RAM, open sockets/ports, users logged on, and running processes. Full Volatile Data

Collection can be lost when the system is shut down or unplugged, thus requiring on-site examination. When a forensic image is not possible for technical or operational reasons, a logical copy of data will be obtained.

23. Special software, methodology and equipment are used to obtain forensic images. Among other things, forensic images normally are “hashed,” that is, subjected to a mathematical algorithm to the granularity of 1038 power, which is an incredibly large number that is much more accurate than the best DNA testing available today. The resulting number, known as a “hash value” confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy. During a logical copy, a hash of each file will be obtained.

24. Forensic Analysis

After obtaining a forensic image or logical copy, the data will be analyzed. Analysis of the data following the creation of the forensic image or logical copy is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user’s computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, email address books, “chat,” instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of the person who used or controlled the computer or storage medium at a relevant time.

25. This affiant is seeking all records of content associated with the TL1 described in Attachment A, that relate to violations of Title 18, United States Code, Section 401(3) (Contempt of Court) and Title 18 Section 157 (Bankruptcy Fraud), including, but not limited to:

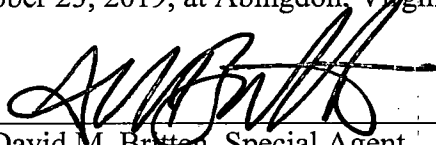
- Any subscriber information, contact information to include, names, addresses, telephone numbers, email addresses or other identifiers;
- Any electronic communication information, including missed, incoming and outgoing communications and any information associated with those electronic communications;

- Any photographs, video and audio files;
- Any text messages, email messages, chats, multimedia messages, installed applications or other electronic communications;
- Any documents, spreadsheets, calendar, note, password, dictionary or database entries;
- Any Global Positioning Satellite (GPS) entries, Internet Protocol Connections, Location entries to include Cell Tower and WiFi entries;
- Any internet or browser entries or history;
- Any system data or configuration information contained within the device
- Any other user or system files and data, contained on the computer itself or an attached peripheral device such as any removable electronic media, which would constitute evidence of violations of law

CONCLUSION

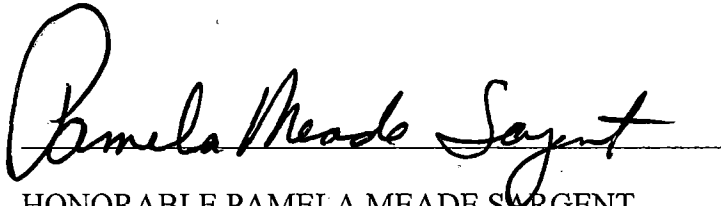
26. Based on the aforementioned factual information and my training and experience in criminal investigations, I submit that probable cause exists to conclude that Russel Louis Geyer, has violated Title 18, United States Code, Section 401(3) (Contempt of Court) and Title 18 Section 157 (Bankruptcy Fraud); and that the search of stored electronic media and communications associated with TL1 will lead to the discovery of evidence of the above aforementioned offenses.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed on October 23, 2019, at Abingdon, Virginia.



David M. Britten, Special Agent
Federal Bureau of Investigation.

SWORN AND SUBSCRIBED TO BEFORE ME
THIS 23RD DAY OF OCTOBER, 2019

A handwritten signature in black ink, reading "Pamela Meade Sargent". The signature is written in a cursive style with a large initial "P" and a long horizontal stroke at the end.

HONORABLE PAMELA MEADE SARGENT
MAGISTRATE JUDGE
UNITED STATES DISTRICT COURT IN THE
WESTERN DISTRICT OF VIRGINIA

Attachment A

This affiant is seeking all records of content associated with Target Laptop 1 (TL1): a black Hewlett-Packard (HP) Laptop with serial number 5CD3483WDF. TL1 is a laptop computer owned by Patricia Geyer and used by Russell Louis Geyer. - that relate to violations of Title 18, United States Code, Section 401(3) (Contempt of Court) and Title 18 Section 157 (Bankruptcy Fraud), including, but not limited to:

Forensic Imaging

An important step that is ordinarily part of an expert's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. This could also require authorities to do on-site examination of the computer systems in order to document any volatile data. Examples of volatile data include, but are not limited to, RAM, open sockets/ports, users logged on, and running processes. Full Volatile Data Collection can be lost when the system is shut down or unplugged, thus requiring on-site examination. When a forensic image is not possible for technical or operational reasons, a logical copy of data will be obtained.

Special software, methodology and equipment are used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 1038 power, which is an incredibly large number that is much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy. During a logical copy, a hash of each file will be obtained.

Forensic Analysis

After obtaining a forensic image or logical copy, the data will be analyzed. Analysis of the data following the creation of the forensic image or logical copy is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry

information, configuration files, user profiles, e-mail, email address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of the person who used or controlled the computer or storage medium at a relevant time.

- Any subscriber information, contact information to include, names, addresses, telephone numbers, email addresses or other identifiers;
- Any electronic communication information, including missed, incoming and outgoing communications and any information associated with those electronic communications;
- Any photographs, video and audio files;
- Any text messages, email messages, chats, multimedia messages, installed applications or other electronic communications;
- Any documents, spreadsheets, calendar, note, password, dictionary or database entries;
- Any Global Positioning Satellite (GPS) entries, Internet Protocol Connections, Location entries to include Cell Tower and WiFi entries;
- Any internet or browser entries or history;
- Any system data or configuration information contained within the device
- Any other user or system files and data, contained on the computer itself or an attached peripheral device such as any removable electronic media, which would constitute evidence of violations of law